UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,804	12/14/2000	James F. Dray JR.	NIST-31	5667

7590 06/04/2004

Michael de Angeli
60 Intrepid Lane
Jamestown, RI 02835

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	7

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,804	DRAY ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art (hereinafter AAPA) in view of Jardin U.S. Pat. No. 6671810 (hereinafter Jardin).

4. As per claim 1, AAPA discloses a method for communicating a document from a sender to a recipient, wherein the recipient is enabled to verify the contents of the document, comprising the steps of: defining a format for document transmission in a document representation language suitable for processing documents including both text and operable code (AAPA: page 3 line 1 – page 4 line 29), employing said format to generate an encoded message, said message including a version of said document that is encoded according to the sender's private key (AAPA: page 7 lines 15-36), includes an identification of the sender, and also includes one of (a) an algorithm for decoding the document according to a private key known only to the sender (AAPA: page 7 lines 15-36), and transmitting said document; and at a receiving location: receiving the encoded message (AAPA: page 7 lines 15-36); employing

the identity of the sender to obtain a public key corresponding to said private key and said decoding algorithm (AAPA: page 7 lines 15-36); and employing said public key and the decoding algorithm to decode the document to verify its contents (AAPA: page 7 lines 15-36). AAPA does not explicitly disclose said format including either (a) an algorithm for encoding the document according to a private key known only to the sender, or (b) a link to a site providing an algorithm for so processing the document; at a transmitting location; and the encoded message include a link to a site providing an algorithm for so decoding the document. However, Jardin discloses communicating encrypted data along with link to encrypting/decrypting algorithms so the client is not required to have existing program for decrypting the data (Jardin: column 1 line 62 – column 3 line 14 and abstract). It would have been obvious to one having ordinary skill in the art to include a link within a message so that encryption/decryption can be achieved dynamically. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Jardin within the system of AAPA because it provides a more robust, secure, and scalable security model not bound by a single security algorithm.

5. As per claim 3, AAPA as modified discloses the method of claim 1. AAPA further discloses wherein said encoding and decoding algorithms collectively perform the following steps: collecting the elements of the host document into a data structure that represents the canonical form of the document at the time of signature (AAPA: page 4 lines 13-22); reducing the canonical data structure into a bit sequence suitable for processing by an electronic signature algorithm (AAPA: page 4 lines 13-22); obtaining a cryptographic key (AAPA: page 4 lines 13-

22); passing the bit sequence and key material to an electronic signature algorithm (AAPA: pages 4-5), which then provides a suitably encoded message (AAPA: pages 4-5); retrieving the output of the signature algorithm (AAPA: pages 4-5); notifying human users of the :results of signature verification processes (AAPA: pages 4-5); and passing the signature and signed data to host applications (AAPA: pages 4-5).

6. As per claim 5, a method for communicating an encrypted message from a sender to a recipient, comprising the steps of: employing a secret: key unique to the sender to encrypt the message (AAPA: page 7 lines 15-36), using a known encryption algorithm having a corresponding known decryption algorithm (AAPA: page 7 lines 15-36); transmitting the encoded message to the recipient (AAPA: page 7 lines 15-36); and separately transmitting the secret key to the recipient (AAPA: page 5 lines 28-29).

AAPA does not explicitly disclose the encoded message includes a language permitting executable software instructions to be embedded in a message also including data, and employing a message format including the decryption algorithm, or a link to a site providing the decryption algorithm, as executable instructions, and the encoded message as data; and employing the decryption algorithm embedded in the message or the link to a site providing the algorithm and the secret key to decrypt the message. However, Jardin discloses dynamically link security algorithm to the encrypted data requested by the client (Jardin: abstract and column 1 line 62 – column 3 line 14). It would have been obvious to one having ordinary skill in the art to include a link within a message so that encryption/decryption can be achieved dynamically. Therefore, it would have been obvious to one having ordinary skill in

the art to combine the teachings of Jardin within the system of AAPA because it provides a more robust, secure, and scalable security model not bound by a single security algorithm.

7. Claims 2, 6, and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Jardin and further in view of Dickinson "This Fall-File Patent Application via Internet" (hereinafter Dickinson).

8. As per claim 2, AAPA as modified discloses the method of claim 1. AAPA as modified further discloses using web-compatible format (AAPA: pages 3-4). AAPA does not explicitly discloses wherein said template includes definition of fields for user insertion of specific information, and said encoded message includes definition of said fields and information placed therein by a user. However, Dickinson discloses that limitation (Dickinson: **section** Instructions for completing the USPTO certificate action form). It would have been obvious to one having ordinary skill in the art to combine the teachings of Dickinson within the combination of AAPA-Jardin because is well known in the art to provide definition of fields for user insertion on web page.

9. As per claim 6, AAPA as modified discloses the method of claim 5. AAPA as modified further discloses using web-compatible format (AAPA: pages 3-4) and security algorithm is dynamically linked to the data (Jardin: column 1 line 62 – column 3 line 14).
AAPA does not explicitly disclose wherein said message format is defined by provision of a template wherein the algorithm is provided as part of a cipher management program, said

template accepting application-specific elements such as the message to be transmitted. However, Dickinson discloses template accepting application-specific elements such as the message to be transmitted (Dickinson: **section** Instructions for completing the USPTO certificate action form). It would have been obvious to one having ordinary skill in the art to combine the teachings of Dickinson within the combination of AAPA-Jardin because is well known in the art to provide definition of fields for user insertion on web page.

10. As per claim 7, AAPA as modified discloses the method of claim 6. AAPA as modified further discloses wherein said cipher management program performs the following functions: Collects the elements of the message to be communicated into a data structure that represents the canonical form of the document (AAPA: page 4 lines 15-22); Reduces the canonical data structure into a bit sequence suitable for processing by a cryptographic algorithm (AAPA: page 4 lines 15-22); Obtains the secret key (AAPA: page 4 lines 15-22); Passes the bit sequence and key material to a cryptographic algorithm (AAPA: pages 4-5); Retrieves the output of the cryptographic algorithm (AAPA: pages 4-5); Notifies a user of the results of encryption/decryption processes (AAPA: pages 4-5); and Passes the plaintext or ciphertext data to host applications (AAPA: pages 4-5).

11. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view of Dickinson and further in view of Jardin.

12. As per claim 4, AAPA discloses a method for employing self-signing document objects (SSDOs) for communication of messages capable of verification by a recipient, comprising the steps of: defining a Template SSDO (T-SSDO) containing an embedded electronic signature processing and verification program, and which is capable of accepting application specific additional elements (AAPA: page 4 lines 13-22); (1) collects and encodes the elements of the P-SSDO into a data structure including the elements of the P-SSDO in a predefined sequence (AAPA: page 4 lines 13-22), (2) decomposes the data structure representing the P-SSDO into a linear sequence of bits (AAPA: page 4 lines 13-22), (3) retrieves the user's private signature key (AAPA: page 4 lines 13-22), and (4) generates and returns an electronic signature, referred to as an S-SSDO, responsive to said linear series of bits, said private key, and a predetermined algorithm (AAPA: page 4 lines 13-22); storing the S-SSDO for subsequent verification; transmitting the S-SSDO to the intended recipient (AAPA: page 4 lines 13-22); and executing the signature verification program, by: (1) recreating the data structure (AAPA: pages 4-7), (2) decomposing the data structure to generate a bit sequence (AAPA: pages 4-7), (3) retrieving the signer's public key information (AAPA: pages 4-7); and (4) employing the bit sequence, signature data, and signer's public key material to verify the origin and structural integrity of the P-SSDO (AAPA: pages 4-7).

AAPA does not explicitly disclose adding application-specific elements to the T-SSDO, to create a Fabricated SSDO (F-SSDO; making the F-SSDO available to a user, such that the user can retrieve and interact with the F-SSDO, resulting in a Processed SSDO (P-SSDO); permitting the user to electronically sign the P-SSDO, causing execution of the embedded signature processing program, in response to which the signature processing program.

However, Dickinson discloses these limitations (Dickinson: **section** Instruction for completing the USPTO certificate action form). It would have been obvious to one having ordinary skill in the art to combine the teachings of Dickinson within the system of AAPA because is well known in the art to provide definition of fields for user insertion on web page and later encrypt the data.

AAPA as modified does not explicitly disclose the algorithm is embedded in the S-SSDO. However, Jardin discloses dynamically link security algorithm to the encrypted data and transmit it to the client (Jardin: abstract and column 1 line 62 – column 3 line 14). It would have been obvious to one having ordinary skill in the art to include a link within a message so that encryption/decryption can be achieved dynamically. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Jardin within the combination of AAPA-Dickinson because it provides a more robust, secure, and scalable security model not bound by a single security algorithm.

13. As per claim 8, AAPA discloses a method for employing self-encrypting document objects (SEDOs) for communication of encrypted messages capable of decryption by a recipient, comprising the steps of: defining a Template SEDO (T-SEDO) containing an embedded cipher management program, and which is capable of accepting application-specific additional elements (AAPA: page 4 lines 13-22); (1) collects and encodes the elements of the P-SEDO into a data structure including the elements of the P-SEDO in a predefined sequence (AAPA: page 4 lines 13-22), (2) decomposes the data structure representing the P-SEDO into a linear sequence of bits (AAPA: page 4 lines 13-22), (3) retrieves the user's secret encryption key (AAPA: page 4 lines

13-22), and (4) generates and returns an encrypted form of the P-SEDO (AAPA: page 4 lines 13-22), referred to as an E-SEDO, responsive to said linear series of bits, said secret encryption key, and a predetermined algorithm (AAPA: pages 4-7); storing the E-SEDO for subsequent verification (AAPA: pages 4-7); transmitting the E-SSDO to the intended recipient (AAPA: pages 4-7); and executing the decryption program (AAPA: pages 4-7), by: (1) recreating the data structure (AAPA: pages 4-7), (2) decomposing the data structure to generate a bit sequence (AAPA: pages 4-7), (3) retrieving the signer's secret encryption key information (AAPA: pages 4-7); and (4) employing the bit sequence and signer's secret encryption key material to decrypt the E-SEDO (AAPA: pages 4-7).

AAPA does not explicitly disclose adding application-specific elements to the T-SEDO, to create a Fabricated SSDO (F-SEDO); making the F-SEDO available to a user, such that the user can retrieve and interact with the F-SEDO, resulting in a Processed SEDO (P-SEDO); permitting the user to indicate a desire to encrypt the P-SEDO, causing execution of the embedded cipher management program, in response to which the cipher management program. However, Dickinson discloses these limitations (Dickinson: **section** Instruction for completing the USPTO certificate action form). It would have been obvious to one having ordinary skill in the art to combine the teachings of Dickinson within the system of AAPA because is well known in the art to provide definition of fields for user insertion on web page and later encrypt the data.

AAPA as modified does not explicitly disclose the security algorithm is embedded in the E-SEDO. However, Jardin discloses dynamically link security algorithm to the encrypted data and transmit it to the client (Jardin: abstract and column 1 line 62 – column 3 line 14). It

would have been obvious to one having ordinary skill in the art to include a link within a message so that encryption/decryption can be achieved dynamically. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Jardin within the combination of AAPA-Dickinson because it provides a more robust, secure, and scalable security model not bound by a single security algorithm.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Douglas et al. U.S. Pat. No. 6223287 discloses dynamically generate a set of encryption information and a token identifying this particular set of encryption information and the information is then sent with the requested program and the communication is achieved in HTTPS protocol (abstract and column 2).

Finley U.S. Pat. No. 5742686 discloses dynamic encryption of information (column 2 line 9 – column 4 line 14).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100